Intra University Cyber Drill 2022

This was the second CTF competation between university students organized by BD-CIRT.

Basic

Basic - 1:50

nc 43.229.15.116 9500
The format for flag is UNICTF2022{flag}

Forensic

Forensic - 1:100

This artifact is same for all question under Forensic Section.
Your first Flag is given in the university cyber drill poster, use it well?
No space in the flag.
The format for this flag is UNICTF2022{flag}

Forensic - 2:50

MD5 hash of the dump file?
The format for this flag is UNICTF2022{flag}

Forensic - 3:50

Most appropriate profile for this machine?
The format for this flag is UNICTF2022{flag}

Incident Response

Scenario and artifacts are same for all questions under Incident Response Section.

Scenario

Onlinepro LLC recently launched their product selling platform "onlinepro.com". But their Devops team have encountered a problem with their site's reachability issue and found some hardware related issue which causes unexpected shutdown of their server. In the meantime, one day their customer support department received a complain from a customer about overcharging for an item. The customer support department raised this issue to the IT department with utmost priority since they have a good reputation in the market.

IT department have been trying to find out the root cause. After initial analysis, they have suspected unauthorized access in their web server. Being unable to find out the exact issue, they are seeking consultation from the experts of a renowned incident response service provider. The artifacts is provided for further analysis and find the flags for this Incident Response section.

Artifact Credential

Zip Password: *7a52d3646477e7f929dca640783182c48133509768a3462e0de817d472d939f9*

VM Credential

Username: *jason*
Password: *cyberrange22*

Incident Response - 1 - The Great Kali : 50

What is the ip address of the attacker when he got initial access to the server?
The format for this flag is UNICTF2022{x.x.x.x}

Incident Response - 2 - Vulnerability : 100

Which file is used or accessed by the attacker for command execution before initial access to the server?
The format for this flag is UNICTF2022{filename.extension}
Example: UNICTF2022{drill.txt}

Incident Response - 3 - Malicious Action : 200

Which payload is used by the attacker to get initial successful access to the server?
The format for this flag is UNICTF2022{payload}

Incident Response - 4 - Stored : 100

What is the uid of the user through which the attacker get initial access to the server?
The format for this flag is UNICTF2022{numeric_value_of_uid}

Incident Response - 5 - Lateral Movement : 200

Attacker created a system user. When this user was created? What is the name of the user? (GMT+6 & 24 hour format)
The format for this flag is UNICTF2022{mm/dd/yyyy_hh:mm:ss.sss,username}

Incident Response - 6 - Reconnaissance : 300

After getting initial access to the server, attacker run a script for enumeration purpose. Can you find the script name and time of execution. (GMT+6 & 24 hour format)
The format for this flag is UNICTF2022{filename.extension,mm/dd/yyyy_hh:mm:ss.sss}

Incident Response - 7 - Plan or Plain : 300

What is the email address of the customer who raise the complain regarding overcharging?
The format for this flag is UNICTF2022{email_address}
Example: UNICTF2022{abc@email.com}

Incident Response - 8 - PVC : 100

For privilege escalation, attacker downloaded an exploit. Which command was used to download the exploit in the victim server? (mention the full command)
The format for this flag is UNICTF2022{command to download the exploit with URL and file name}

Incident Response - 9 - Second Option : 200

The attacker setup a special type of malware in the victim server. Your task is to identify the malware type.
The format for this flag is UNICTF2022{malwaretype}
Flag Example: UNICTF2022{adware}

Incident Response - 10 - Message Digest : 300

From the victim server, attacker exfiltrated sensitive data and transferred it. what is the md5

hash of the file containing those sensitive data?

The format for this flag is UNICTF2022{md5hashvalue}

Miscellanous

Miscellanous - 1 - Departure : 150

Artifact contain some suspicious code.

The format for flag is UNICTF2022{flag}

Miscellanous - 2 - Demice : 100

Creation of an artifact have a true story.

The format for flag is UNICTF2022{flag}

OSINT

OSINT - 1 - Behind or Beside : 200

This is a nice place. Isn't it? John wrote a review of a nearby location. What is the location of his workplace?

The format for this Flag is: UNICTF2022{location_of_John's_workplace}

Flag Example: UNICTF2022{Hampshire}

Reverse Engineering

Reverse - 1 : 100

This is very easy to find the flag from the given artifact.

The format for flag is UNICTF2022{flag}

Web Vulnerability

Scenario

A renowned organization's mobile app release date got leaked. Few days back a new employee joined in the organization and he has been assigned to develop a web based eCommerce app. The organization has some development server but all are occupied by other teams. Due to unavailability of development server he used production server for develop and testing. After the the incident, the organization initiate a primary investigation of the incident and found that the eCommerce application has some vulnerabilities. Attacker used those vulnerabilities to get inside the server and exfiltrate sensitive data.

The organization wants to know what sensitive data got breach and how? As an incident responder your task is to find out details about the data breach by answering several questions.

Web Vulnerability - 1 : 50

From the attached artifact find the database server version used for the application?

The format for this flag is UNICTF2022{flag}

Web Vulnerability - 2 : 100

From the attached artifact find the password of eCommerce admin user in plain text?
The format for this flag is UNICTF2022{flag}

Web Vulnerability - 3 : 50

Attacker found that application was vulnerable to run system commands. What is the Common Weakness Enumeration (CWE) number for that vulnerability?
The format for this flag is UNICTF2022{CWE-NUMBER}

Web Vulnerability - 4 : 50

During enumeration attacker found a file which contains user credential. Attacker was able to login to the server as a non-system user. What is the name of that user?
The format for this flag is UNICTF2022{flag}

Web Vulnerability - 5 : 200

Try to find out the password of that user from the attached file?
The format for this flag is UNICTF2022{flag}

Web Vulnerability - 6 : 25

What is the Content-Type/MIME of the file which contains credential?
The format for this flag is UNICTF2022{flag}

Web Vulnerability - 7 : 150

Attacker was able to get database privileged user password from application configuration file. What is the password?
The format for this flag is UNICTF2022{flag}

Web Vulnerability - 8 : 75

Attacker export a file from a database using the privileged user. What is the database name and table name?
The format for this flag is UNICTF2022{database:table}

Web Vulnerability - 9 : 50

Attacker used several techniques to exfiltration data of the application. Find out the application name from the artifact?
The format for this flag is UNICTF2022{flag}

Web Vulnerability - 10 : 250

Find out the the release date of the application from the attached artifact?
The format for this flag is UNICTF2022{dd-mm-yyyy}

Prepared by
Sadi Hurayv
IIT, NSTU.